Embedded Intel® Architecture (EIA) in Virtual Private Networks (VPN)

Application Note

February 2000

Order Number: 273337-001

Application Note

Contents

1.0 Overview 5
1.1 Introduction 5
1.2 Benefits of Virtual Private Networks 5
2.0 VPN and EIA Basics 6
2.1 VPN Technology 6
2.2 EIA-Based Hardware Platform 6
3.0 Performance 7
4.0 VPN Solutions 8
4.1 Firewall 8
4.1.1 Firewall Techniques 8
4.2 Protocols 9
5.0 Implementation 9
6.0 System Components 11
6.1 Processor: Intel® Celeron™ Processor 11
6.2 Chipset: Intel® 440BX AGPset 11
6.3 Network Component: Intel® 82559 12
7.0 Operating System, Drivers, and Application Software 12
8.0 Conclusion 13
9.0 Related Resources 13

Figures

1 VPN Software and Hardware 7
2 VPN Reference Configuration Block Diagram 10

Tables

1 VPN Reference Configuration Components 10

1.0 Overview

1.1 Introduction

A virtual private network (VPN) is a private network constructed using public telecommunication infrastructure. VPN is an encrypted or encapsulated communication process that transfers encrypted data over open, unsecured, and routed networks. In the context of this application note, the Internet is the communication medium. The network is called virtual because it is dynamic and connections are set up as and when needed.

Because the network is formed logically regardless of the physical structure of the Internet, the connections making up a VPN do not have the same physical characteristics as hard-wired connections. The reason for fast growth in the VPN arena is that VPN enhances the price and performance of enterprise networks by using the shared public infrastructure for data. This concept is extended to extranets and wide-area Intranets as well.

This application note discusses using an embedded Intel® architecture (EIA) platform for VPN systems. This platform is an open architecture platform and is widely supported. Some of the popular operating systems supported include Microsoft Windows* 95/98/2000/NT, Linux*, Unix*, and Solaris*. A VPN developer can easily develop VPN systems based on EIA.

This application note provides an introduction to implementing a software-based VPN solution on an embedded Intel architecture platform. It describes the platform components and discusses the VPN technologies and protocols.

1.2 Benefits of Virtual Private Networks

A broader variety of communications are supported today than ever before. Other market factors, such as multi-site access, required flexibility, and the increasing number of mobile users are helping to drive up the cost of communications infrastructure. In addition, valuable and sensitive information travels through Internets, extranets, and Intranets, increasing the risk to corporate security. A recent study (FBI/CSI Computer Crime & Security Survey, 1999) shows financial losses due to computer security breaches mounted to over $100 million for a third straight year.

VPN makes possible the interconnection of different corporate network sites, allowing remote users to access the corporate network. VPN provides greater flexibility and scalability. All access can be controlled while reducing cost of service and equipment when compared to methods such as leased lines and long-distance calls. Privacy is achieved through the use of a tunneling protocol and security procedures.

2.0 VPN and EIA Basics

2.1 VPN Technology

VPN ensures data security by combining two or more of the following concepts:

- Authentication: This service prevents unauthorized users from gaining admission to the network. Various password-based and challenge-response systems, hardware-based tokens, and digital certificates can be used to authenticate users on a VPN and control access to network resources. This ensures that data originates at the source that it claims.
- Privacy: Encrypting the data as it travels through the VPN guards the privacy of the travelling information. Data then decrypts to the original information.
- Integrity: Encapsulation in a tunnel, the encapsulated data hides the underlying routing and switching infrastructure of the Internet from both senders and receivers.
- Access Control: Restricting unauthorized users from gaining admission.

2.2 EIA-Based Hardware Platform

Encryption and encapsulation are processing power-intensive. Platform selection is made based on performance and supported features. The major components of a VPN appliance include the processor, chipset, Ethernet controllers, memory, and VPN software. This application note discusses an Intel Celeron™ processor-based system. Two IEEE 802.3 Ethernet/Fast Ethernet ports are provided. In an entry-level appliance, two ports provide the optimum trade-off of flexibility and cost. One Ethernet port is intended for connection to the LAN. The other Ethernet port can connect to a cable modem, xDSL modem, server, or other device. Alternatively, add-in modems and network interface cards for a broad variety of WAN connections (ISDN, T1, v.90, etc.) can be supported with the PCI slots.

Ideally, a VPN appliance is administered remotely on the LAN. However, the described implementation contains an RS-232 serial port to support the use of a local console.

3.0 Performance

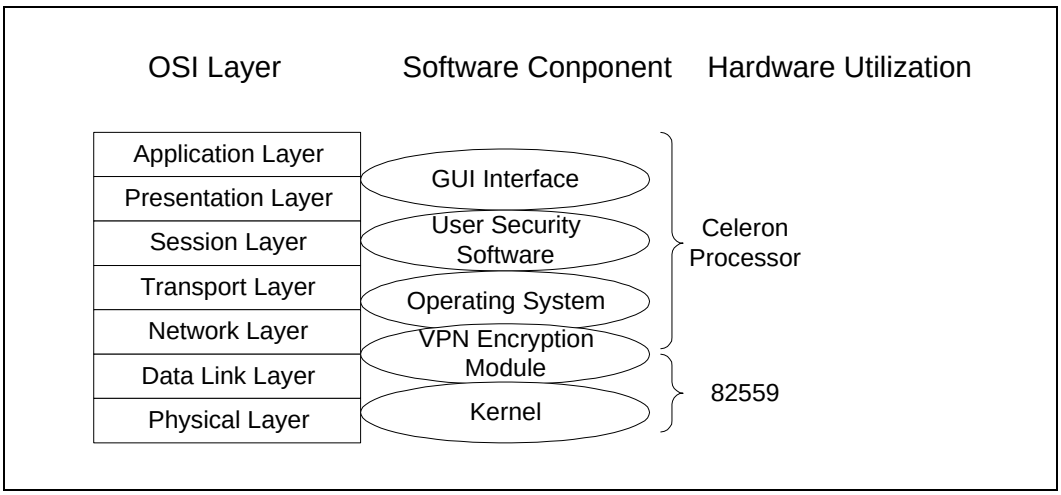
Encryption and encapsulation are processing-intensive, which must be considered when defining performance requirements for a VPN system. For example, 3DES encryption requires 50-100 times the processing power of IP routing, or 60-80% of CPU processing power. When data encryption is needed along with encapsulation, it is recommended that a hardware-based solution be used with an independent processor. This adds to the physical and logical security of the system. Software based systems are limited in performance and are useful only at slower data rates.

Processor speed must be adequate for the number of clients connected and for handling transactions while running multiple TCP stacks. On average, a 300-MHz CPU can sustain 5-8 Mbps network connections, which in total can support 1500-2000 connections.

These numbers vary widely based on the OS and application software used. Because the CPU supports multiple TCP/IP, it is possible to use MMX™ technology instructions and Streaming SIMD Extensions instructions in implementing the stack.

Figure 1 illustrates VPN software components and hardware utilization with an OSI layer.

Figure 1. VPN Software and Hardware



CPU performance is needed to process encryption/decryption algorithms, for VPN management, and to run user software. CPU performance is also needed for simultaneous tunnel connections.

4.0 VPN Solutions

There are three general models of VPN implementation: server-based, router-based, and firewall-based. The system example described in this application note is not limited to any particular implementation model. Rather, it is a dedicated, stand-alone appliance that can be inserted into existing infrastructure.

VPN solutions can be further categorized as software-based solutions and hardware-based solutions. Software VPN systems are available for systems that do not process a lot of traffic. These solutions usually run on existing servers and share resources with them. For mid- to larger-sized solutions, hardware-based solutions are recommended. VPN appliances are especially attractive for small businesses and remote office environments. Firewalls are essential in any VPN. A firewall is the first line of defense in protecting private information in any VPN.

4.1 Firewall

A firewall prevents unauthorized access to or from private networks, especially intranets. Firewalls can be implemented in hardware, software, or a combination of both. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. For greater security, data is often encrypted.

4.1.1 Firewall Techniques

The many firewall techniques include:

- Packet filtering, which looks at each packet entering or leaving the network and accepts or rejects it based on a programmed list of criteria.
- Applications gateways that apply security mechanisms to the applications such as FTP or Telnet servers.
- Circuit-level gateways that apply security when a Transmission Control Protocol (TCP) or User Defined Protocol (UDP) connection is established.
- A proxy server intercepts all messages entering and leaving the network, while hiding the true network addresses.

Like routers, firewalls must process all IP traffic, passing information based on filters defined for the firewall. Firewall-based VPNs are typically best used when frequent reconfiguration is not required. VPN solutions using special hardware designed for tunneling, encryption, and user authentication work well.

4.2 Protocols

The four suggested protocols for creating VPNs over the Internet are:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- IP security protocol (IPSec)

One reason for the numerous protocols is that for some companies, a VPN is a substitute for remote access servers, allowing mobile users and branch offices to dial into the protected corporate network via their local ISP. For others, a VPN may consist of traffic traveling in secure tunnels over the Internet between protected LANs. PPTP, L2F, and L2TP are largely aimed at dial-up VPNs, while the main focus of IPSec has been LAN–to–LAN solutions.

PPTP has been a widely deployed solution for dial-in VPNs. PPTP builds on the functionality of Point-to-Point Protocol (PPP), the most commonly used protocol for remote access to the Internet. PPTP relies on the authentication mechanisms within PPP, namely Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

PPTP is designed to run at Open Systems Interconnect (OSI) Layer 2, or the link layer, as opposed to IPSec, which runs at Layer 3. The limitations of PPTP include a lack of strong encryption for protecting data.

L2F tunnels traffic from users to their corporate sites. L2F is able to work directly with other media and allows tunnels to support more than one connection.

L2TP is a Layer 2 protocol and defines its own tunneling protocol. L2TP uses IPSec's encryption methods.

IPSec allows the sender to authenticate or encrypt each IP packet or apply both operations to the packet. The two methods of using IPSec are transport mode and tunnel mode. In transport mode, only the transport-layer segment of an IP packet is authenticated or encrypted. In tunnel mode, the entire IP packet is authenticated. Since IPSec includes strong security measures, it is often considered the best VPN solution for Internet environments.

5.0 Implementation

The components of a VPN appliance include the processor, chipset, Ethernet controllers, memory, and VPN software. This application note discusses an Intel Celeron processor-based system. Two IEEE 802.3 Ethernet/Fast Ethernet ports are provided. In an entry-level design, two ports provide the optimum trade-off of flexibility and cost. One Ethernet port is intended for connection to the LAN. The other Ethernet port can connect to a cable modem, xDSL modem, server, or other device. Alternatively, add-in modems and network interface cards for a broad variety of WAN connections (ISDN, T1, v.90, etc.) can be supported with the PCI slots.

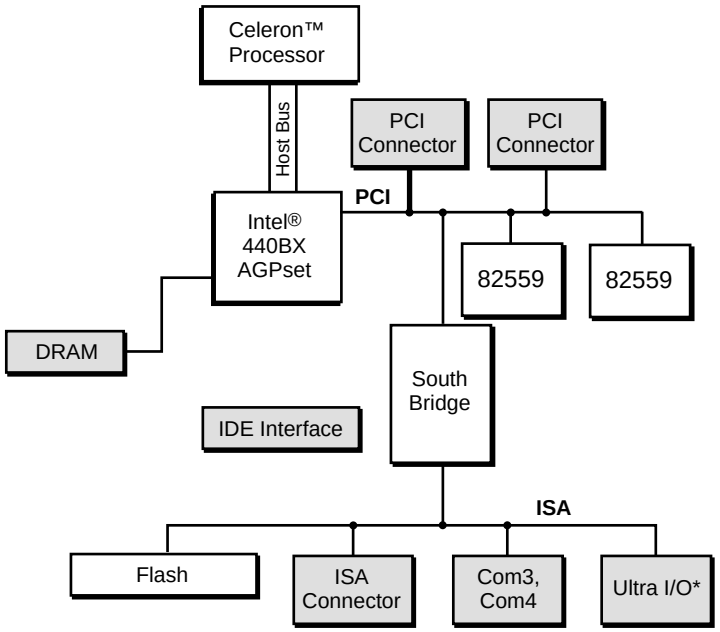
Ideally, a VPN appliance is administered remotely on the LAN. However, the described implementation contains an RS-232 serial port for local console use.

The implementation depicted in Figure 2 enables developers to meet higher performance requirements while addressing today's value-driven market needs. The Intel 440BX AGPset offers a cost-effective way to ensure that current designs will be ready for 100 MHz system bus implementations. This reference configuration provides a cost-effective and optimized networking solution.

Table 1. VPN Reference Configuration Components

	Recommended Component
CPU	Intel® Celeron™ processor at 566 MHz
Chipset	Intel 440BX AGPset
LAN	Intel 82559
Flash	Intel Boot Block and StrataFlash™ Memory

Figure 2. VPN Reference Configuration Block Diagram



Note: Non-Intel components are shown in gray.

A7830-01

6.0 System Components

The following components describe an Intel architecture VPN solution that addresses the unique performance requirements of this application.

6.1 Processor: Intel® Celeron™ Processor

The Intel Celeron processor implements a Dynamic Execution microarchitecture and executes MMX™ media technology instructions for enhanced media and communication performance. The Celeron processor also uses the same multi-transaction system bus used in the Intel Pentium II processor. The Celeron processor supports multiple low-power states such as AutoHALT, Stop-Grant, Sleep, and Deep Sleep to conserve power during idle times. The Celeron processor is based on the P6 core and is provided in a Flip-Chip Pin Grid Array (FCPGA) package for use in entry-level designs. The Celeron processor utilizes the AGTL+ system bus used by the Pentium II processor with support limited to single processor-based systems. The Celeron processor includes an integrated 128-Kbyte level-two cache with a separate 16-Kbyte instruction and 16-Kbyte data level-one caches. The level-two cache is capable of caching 4 Gbytes of system memory address space. Processor utilization is important for performing encryption/decryption processes.

For additional Celeron processor information, please refer to the following URL:

http://developer.intel.com/design/celeron/datashts/243658.htm

6.2 Chipset: Intel® 440BX AGPset

The Intel 440BX AGPset is the chipset supporting the Intel Celeron processor with a 66-MHz system bus and 100-MHz SDRAM. As Intel's second-generation AGPset with Intel Quad Port Acceleration (QPA), the Intel 440BX AGPset improves the speed of the system bus from 66 MHz to 100 MHz, while increasing the width and depth of buffers to the system bus, Accelerated Graphics Port (AGP), SDRAM, and PCI bus. In addition, the 440BX AGPset can interface with ATA/66 HDD in UDMA mode 2.

The 82443BX has the following features:

- Support for single Celeron processor configuration
- 64-bit GTL+ based Host Bus interface
- 32-bit Host address support
- 64-bit main memory Interface with optimized support for SDRAM at 100 and 66/60 MHz
- 32-bit Primary PCI Bus Interface (PCI) with integrated PCI arbiter
- Extensive Data Buffering between all interfaces for high throughput and concurrent operations
- "*Deep Green*" desktop power management support

For additional information on the Intel 440BX AGPset, please refer to the following URL:

http://developer.intel.com/design/chipsets/440bx/

6.3 Network Component: Intel® 82559

The 82559 is Intel's second generation, fully integrated 10BASE-T/100BASE-TX LAN solution. The 82559 consists of both the Media Access Controller (MAC) and the physical layer (PHY) interface combined into a single component solution. The combined component is packaged in a 15 mm x 15 mm, 196-lead, thin BGA package. The 82559 provides 32-bit PCI bus high-speed data transfer without additional glue logic. Its bus master capabilities enable the component to process high level commands and perform multiple operations, which lowers CPU utilization by off-loading communication tasks from the CPU. CPU utilization is just as important as network throughput because the CPU needs considerable processing power to execute the tunneling encryption/decryption algorithm.

The 82559 also includes an interface to a serial (4-pin) EEPROM and a parallel interface to a 128-Kbyte Flash memory. The EEPROM provides power-on initialization for hardware and software configuration parameters. The parallel port can be used as either a Flash memory interface or an ISA-like interface for a modem. Combined with a Total Cost of Ownership (TCO) controller, the 82559 can help reduce the total cost of ownership in network environments. The device includes a System Management Bus (SMB) interface enabling the TCO controller to communicate with a management agent on the network. For details on Intel 82559, please refer to the following URL:

http://developer.intel.com/design/network/82559.htm.

7.0 Operating System, Drivers, and Application Software

VPN systems can be designed to use a variety of operating systems. In this reference design, Linux is selected as the operating system due to its cost, its open configuration model, and a small system footprint.

To jump start the LAN interface in your VPN appliance design, Intel offers a free Linux driver for the 82559 Ethernet controller on its web site. See Intel's Software Assistant at the following URL:

http://amber.intel.com/scripts-qcube/software/softgridb.asp

Today, there are many VPN software solutions. Many of them are proprietary and are linked to a particular vendor's hardware or router software. Systems based on this reference design are more likely to be running standards-based software conforming to specifications such as the Internet Engineering Task Force's (IETF) Internet Protocol Security (IPSEC) or the proposed L2TP standard.

8.0 Conclusion

Internet-based VPNs enhance the price and performance of enterprise networks, extranets, and wide-area Intranets. VPNs rely on CPU performance to for processing encryption/decryption algorithms, VPN management, user software, and for simultaneous tunnel connections. The features and performance of the Celeron processor make it well suited for VPN systems. VPN systems are easily implemented using EIA processors.

9.0 Related Resources

Refer to the following web sites for additional information on VPN.

- http://developer.intel.com/
- *VPNWorx Quick Reference Guide* (Lucent Technologies) http://www.lucent.com/vpnworx/vpnworxresource.html
- http://www.ietf.org/